

Notice of Allowability

Application No.

09/896,851

Examiner

Justin Darrow

Applicant(s)

MCGARVEY, JOHN R.

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to telephone conversation with Mr. Robert Showalter on July 10, 2006.
2. ☒ The allowed claim(s) is/are 1-14, 18-27 and 29.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) ☐ All b) ☐ Some* c) ☐ None of the:
 1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
 5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
 - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
 - (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mr. Robert Showalter on July 10; 2006. The application has been amended as follows:

In the Claims: Please enter attached claim set.

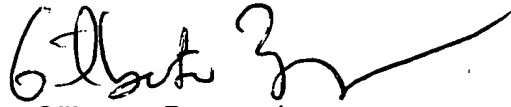
2. The following is an examiner's statement of reasons for allowance: The prior art failed to disclose having a Kerberos protocol for authenticating a client and then generating a second message using a Public Key Infrastructure authentication protocol. The instant amendments were made strictly to ensure that the system for authentication of messages is implemented using a processor in accordance with the disclosure at page 10, describing Figure 3.

The amendments to claims 1, 27 and 29 were made to avoid any conflict with recently discovered patent to McGarvey, 6,643,774 and cited herein. The amendments also conform claims 1, 27 and 29 with the other independent claims 18, 19 and 21.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Art Unit: 2132

Any inquiry concerning this communication should be directed to Gilberto Barron Jr. at telephone number 571-272-3799.



Gilberto Barron Jr.
SPE
Art Unit 2132

for

Justin Darrow
Primary Exam 2132

Art Unit: 2132

1. (Currently Amended) A method of authenticating a message from a client using a first authentication protocol to a resource manager using a second authentication protocol different from the first authentication protocol, the method comprising:

generating a second message from the message from the client, the second message including information from the client which has been authenticated using the first authentication protocol;

authenticating the second message using the second authentication protocol;
and

providing the authenticated second message to the resource manager[.] wherein the first authentication protocol comprises Kerberos and the second authentication protocol comprises public key infrastructure (PKI).

2. (Cancelled).

3. (Currently Amended) The method of Claim [2] 1, wherein the step of authenticating the second message comprises signing the second message with a private key corresponding to a PKI certificate available to the resource manager so as to provide the second message with a signature.

4. (Original) The method of Claim 3, wherein the step of generating a second message comprises:

receiving a Kerberos ticket;

verifying authenticity of the Kerberos ticket;

extracting principal information from the Kerberos ticket if the authenticity of the ticket is verified; and

generating the second message utilizing the extracted principal information.

5. (Original) The method of Claim 4, wherein the step of generating the second message utilizing the extracted principal information comprises incorporating the principal information with data from the message from the client to provide the second message.

6. (Original) The method of Claim 5, wherein the resource manager carries out the steps of:

receiving the second message;

authenticating the signature of the second message;

extracting the principal information from the second message; and

processing the data from the second message based on the principal information from the second message if the signature of the second message is authentic.

7. (Original) The method of Claim 4, wherein the step of generating the second message utilizing the extracted principal information comprises generating at least a first component and a second component of the second message, the first component containing the principal information and the second component containing data from the message from the client.

8. (Original) The method of Claim 7, wherein the step of signing the second message with a private key comprises signing the first component with the private key and signing the second component with the private key.

9. (Original) The method of Claim 8, wherein the resource manager carries out the steps of:

receiving the at least two second messages,
authenticating the signatures of the second message;
extracting the principal information from the first component;
extracting the data from the second component; and
processing the data of the second component based on the principal
information from the first component if the signatures of the at least two second
messages are authentic.

10. (Original) The method of Claim 4, wherein the step of receiving a Kerberos ticket
comprises receiving a Kerberos service ticket from a middle-tier server.

11. (Original) The method of Claim 10, wherein the step of providing the authenticated
second message to the resource manager comprises returning the authenticated
second message to the middle-tier server.

12. (Original) The method of Claim 11, wherein the Kerberos service
ticket and the authenticated second message are encrypted.

13. (Original) The method of Claim 10, wherein the Kerberos service
ticket is obtained by the middle-tier server responsive to receiving a delegatable
Kerberos ticket.

14. (Original) The method of Claim 10 further comprising incorporating
an identification of the middle-tier server in the second message.

15-17. (Canceled).

Art Unit: 2132

18. (Previously Amended) A method of providing authentication for communications between a Kerberos client and a public key infrastructure (PKI) server, the method comprising:

- authenticating a message from the Kerberos client at a party trusted by the PKI server;

- signing the authenticated message with the PKI private key of the party trusted by the PKI server;

- forwarding the signed authenticated message to the PKI server; and

- incorporating an identification of a principal of the message from the Kerberos client with the signed authenticated message, wherein the step of incorporating an identification of the principal of the message comprises incorporating the identification of the principal into a second message signed with the private key, and wherein forwarding the signed authenticated message comprises forwarding the signed authenticated message and the second message to the PKI server.

19. (Previously Amended) A method of providing authentication for communications between a Kerberos client and a public key infrastructure (PKI) server, the method comprising:

- authenticating a message from the Kerberos client at a party trusted by the PKI server;

- signing the authenticated message with the PKI private key of the party trusted by the PKI server; and

forwarding the signed authenticated message to the PKI servers, wherein the step of authenticating the message is performed responsive to receiving a Kerberos service ticket.

20. (Original) The method of Claim 19, further comprising incorporating an identification of a source of the Kerberos service ticket with the signed authenticated message.

21. (Currently Amended) A system for authentication of messages from a client utilizing Kerberos authentication and a resource manager utilizing public key infrastructure (PKI) authentication, comprising:

a data processor apparatus implementing a public key signature service
configured to receive a Kerberos service ticket,
authenticate the Kerberos service ticket,
generate a message incorporating data associated with the authenticated Kerberos service ticket which is signed using a digital signature based on a PKI private key and PKI certificate so as to allow the resource manager to authenticate the message and provide the signed message to the resource manager.

22. (Original) The system of Claim 21, wherein the public key signature service is further configured to extract principal information from the Kerberos service ticket and incorporate the principal information with the message.

23. (Original) The system of Claim 21, further comprising a middle-tier server configured to obtain the Kerberos service ticket responsive to receipt of a delegatable Kerberos ticket and to provide the obtained Kerberos service ticket to the public key signature service.

Art Unit: 2132

24. (Original) The system of Claim 23, wherein the public key signature service is further configured to provide the signed message to the resource manager by returning the signed message to the middle-tier server and wherein the middle-tier server is further configured to forward the signed message returned by the public key signature service to the resource manager.

25. (Original) The system of Claim 24, wherein the public key signature service is further configured to extract middle-tier server information from the Kerberos service ticket and incorporate the middle-tier server information with the message.

26. (Original) The system of Claim 22, wherein the public key signature service is further configured to selectively incorporate the principal information into the message with the data associated with the Kerberos service ticket and to selectively generate a second message associated with the message containing the data associated with the Kerberos ticket which contains the principal information and sign the message containing the data and the second message if the second message is generated.

27. (Currently Amended) A system for authenticating a message from a client using a first authentication protocol and a resource manager using a second authentication protocol different from the first authentication protocol, comprising:

means for generating a second message from the message from the client, the second message including information from the client which has been authenticated using the first authentication protocol;

means for authenticating the second message using the second authentication protocol; and

means for providing the authenticated second message to the resource manager[.] wherein the first authentication protocol comprises Kerberos and the second authentication protocol comprises public key infrastructure (PK1).

28. (Canceled).

29. (Currently Amended) A computer program product for authenticating a message from a client using a first authentication protocol and a resource manager using a second authentication protocol different from the first authentication protocol, comprising:

a computer readable storage media having computer readable program code embodied therein, the computer readable program code comprising:

computer readable program code which causes a computer to generate a second message from the message from the client, the second message including information from the client which has been authenticated using the first authentication protocol;

computer readable program code which causes the computer to authenticate the second message using the second authentication protocol; and

computer readable program code which causes the computer to provide the authenticated second message to the resource manager [.] wherein the first authentication protocol comprises Kerberos and the second authentication protocol comprises public key infrastructure (PK1).

30. (Canceled).